UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/693,605	10/20/2000	Ashraf Madoukh	15247.6	8437

21129 7590 07/14/2006

SPENCER, FANE, BRITT & BROWNE
1000 WALNUT STREET
SUITE 1400
KANSAS CITY, MO 64106-2140

EXAMINER	
SHERKAT, AREZOO	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 07/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/693,605	MADOUKH ET AL.	
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 May 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28 and 40-70* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28 and 40-70* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 October 0200* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Response to Amendment

This office action is responsive to Applicant's amendment received on 5/1/2006. claims 1 and 28 are amended. Claims 29-39 and 71-97 are cancelled. Claims 1-28 and 40-70 are pending.

Response to Arguments

Applicant's arguments, see Remarks, filed 5/1/2006, with respect to the rejection(s) of claim(s) 1-28 and 40-70 under 35 U.S.C. 102(b) have been fully considered and are persuasive with regard to some of the claims. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of newly discovered prior art U.S. Patent No. 5,604,801 to Dolan et al..

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-2, 5-8, 10-13, 16-28, 40-45, 47-52, 54-57, and 63- 66, are rejected under 35 U.S.C. 102(b) as being anticipated by Linehan et al., (U.S. Patent No. 5,495,533 and Linehan hereinafter).

Claims 1-2, 5-8, 10-13, 16-28, 40-45, 47-52, 54-57, and 63- 66, are rejected under 35 U.S.C. 102(b) as being anticipated by Linehan et al., (U.S. Patent No. 5,495,533 and Linehan hereinafter).

Regarding claims 1, 6-8, 10, 17-21, 26-28, and 40-44, Linehan discloses a computer readable medium containing a database structure for storage of encrypted data, the database structure comprising: at least one data entity encrypted by at least one encryption key, the data entity having at least one searchable attribute, and at least one encryption key identification stored (col. 9, lines 19-24) in association with the data entity and corresponding to the encryption key (col. 7, lines 30-67 and col. 4, lines 1-26).

Regarding claims 2, 5, 11, 13, 16, 22, 24-25, 45, 47, 49-50, and 66 Linehan discloses wherein the at least one encryption key identification is encrypted by a system key (i.e., control key), and the database structure further comprises a system key common name corresponding to the system key, the system key common name being stored in association with the data entity (i.e., the database contains an entry for each control key that has been generated. The database entries are indexed by control key index numbers)(col. 9, lines 10-59).

Regarding claims 12, 63 and 65, Linehan discloses wherein the data entity and encryption key identification are stored in a first database (i.e., personal key client), and

further comprising storing the encryption key in a second database (i.e., personal key database/server)(col. 9, lines 10-59).

Regarding claims 51-52, 55-57, and 64, Linehan discloses further comprising checking for expiration of the system key, and upon expiration of the system key, discontinuing use of the system key and generating and using a new system key (Col. 8, lines 65-67 and Col. 9, lines 1-10).

Regarding claims 70, Linehan discloses a method for storage and retrieval of encrypted data, the method comprising:

encrypting a plurality of data entities with a rotating and dynamic encryption key having an encrmtion key identification, storing the data entities, and creating and rotating to a new encryption key upon occurrence of a desired rotation event (Col. 8, lines 65-67 and Col. 9, Lines 1-58).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 14-15, 23, 46, and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Linehan et al., (U.S. Patent No. 5,495,533 and Linehan hereinafter), in view of Dolan et al., (U.S. Patent No. 5,604,801 and Dolan hereinafter).

Regarding claims 14-15 and 46, Linehan does not expressly disclose wherein the system key is stored on a security token such as a smart card reader.

However, Dolan discloses wherein the system key is stored on a security token such as a smart card and is in possesion of the user (col. 5, lines 20-53).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Linehan with teachings of Dolan because it would allow to include storing the system key in a security token such as a smart card as suggested by Dolan. One of ordinary skill in the art would have been motivated by the suggestion of Dolan to control the public key processing by providing the server with a key to enable the server to decrypt the private key, use it, and delete the private key after use (Dolan, col. 3, lines 21-26).

Regarding claims 23 and 48, Linehan discloses wherein a network authentication mechanism could be based upon public-key cryptography (col. 3, lines 32-37).

Moreover, Dolan discloses wherein encrypting the encryption key identification with a system key comprises encrypting the encryption key identification with a system public key (col 5, lines 60-67 and col. 6, lines 1-25).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Linehan with teachings of Dolan because it would allow to include wherein encrypting the encryption key identification with a system key comprises encrypting the encryption key identification with a system public key as suggested by Dolan. One of ordinary skill in the art would have been motivated by the suggestion of Dolan to control the public key processing by providing the server with a key to enable the server to decrypt the private key, use it, and delete the private key after use (Dolan, col. 3, lines 21-26).

Claims 3-4, 9, 53-54, 58-59, and 67-69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Linehan et al., (U.S. Patent No. 5,495,533 and Linehan hereinafter), in view of Kaufman et al., (U.S. Patent No. 5,764,772 and Kaufman hereinafter).

Regarding claims 3-4, 9, and 53, Linehan discloses wherein the system key common name is hashed, and the data structure further comprising a system key common name hash value (i.e., system key index numbers) stored in association with the system common name (Col. 9, lines 10-25).

Linehan does not expressly disclose wherein the system key common name is hashed, and the data structure further comprising a system key common name hash value stored in association with the system common name.

However, Kaufman discloses wherein the system key common name is hashed, and the data structure further comprising a system key common name hash value stored in association with the system common name (Col. 8, lines 20-67 and Col. 9, lines 1-63).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Linehan with teachings of Kaufman because it would allow to include wherein the system key common name is hashed, and the data structure further comprising a system key common name hash value stored in association with the system common name with the motivation to make it impossible to make an undetected modification to the encrypted key field once the encrypted message was generated (Kaufman, Col. 10, lines 20-37).

Regarding claims 54, 58-59, and 67-69, Linehan discloses a computer readable medium containing a database structure for storage of encrypted data, the database structure comprising: at least one data entity encrypted by at least one encryption key, the data entity having at least one searchable attribute, and at least one encryption key identification in association with the data entity and corresponding to the encryption key (Col. 7, lines 30-67 and Col. 4, lines 1-26), and requesting a data manipulation using a searchable attribute, searching for matches to the searchable attribute (Col. 7, lines 54-67 and Col. 8, lines 8-17), searching for the system key common name, searching for the system key using the system key common name, decrypting the encryption key identification with the system key, searching for the encryption key using the encryption

key identification, and decrypting the data entity with the encryption key (Col. 9, lines 10-58).

Linehan does not expressly disclose searching for the system key common name using the system key hash value.

However, Kaufman discloses wherein the system key common name is hashed, and the data structure further comprising a system key common name hash value stored in association with the system common name (Col. 8, lines 20-67 and Col. 9, lines 1-63).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Linehan with teachings of Kaufman because it would allow to include wherein the system key common name is hashed, and the data structure further comprising a system key common name hash value stored in association with the system common name with the motivation to make it impossible to make an undetected modification to the encrypted key field once the encrypted message was generated (Kaufman, Col. 10, lines 20-37).

Claims 60-62 are rejected under 35 U.S.C. 103(a) as being unpatentable over Linehan et al., (U.S. Patent No. 5,495,533 and Linehan hereinafter), in view of Kaufman et al., (U.S. Patent No. 5,764,772 and Kaufman hereinafter), in further view of Alegre et al., (U.S. Patent No. 6,199,113 and Alegre hereinafter).

Regarding claims 60-62, Linehan does not expressly disclose further comprising generating a new encryption key for each user action.

However, Alegre discloses further comprising generating a new encryption key for each user action (i.e., session keys with expiration criteria)(Col. 5, lines 7-67 and Col. 6, lines 1-50).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Linehan and Kaufman with the teachings of Alegre because it would allow to include generating a new encryption key for each user action with the motivation to allow access by users on the Internet in a controlled and secure manner and to better prevent breach of security and improper access to resources (Alegre, Col. 2, lines 24-35).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

A. Sherkat

Arezoo Sherkat
Patent Examiner
Group 2131
July 10, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100